AMENDMENTS TO THE CLAIMS

1-34. **(Canceled)**

35. **(New)** A copyright protection system comprising:

a recording apparatus configured to encrypt a content and to record the encrypted content;

a recording medium on which the encrypted content is recorded; and

a plurality of reproduction apparatuses, each of which is configured to read out and decrypt the encrypted content recorded on said recording medium,

wherein each of said plurality of reproduction apparatuses is one of either a first plurality of reproduction apparatuses which belong to a first category and hold plural device keys and information regarding generation of the plural device keys or a second plurality of reproduction apparatuses which belong to a second category and hold only one device key,

said recording apparatus is configured (a) to generate, for said plurality of reproduction apparatuses and based on a media key and the device key held by each of said plurality of reproduction apparatuses, a plurality of revocation data intended for revoking a device key held by a specific reproduction apparatus of a respective category, (b) to generate the encrypted content which is the content encrypted based on the media key, and (c) to record the plurality of revocation data, the information regarding the generation of the device keys for generating the plurality of revocation data, and the encrypted content onto said recording medium,

the first plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said first plurality of reproduction apparatuses, the information regarding the generations of the plural device keys, and the encrypted content, and (b) to decrypt the encrypted content based on the plurality of revocation data read out and the information regarding the generation of the plural device keys, and

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said second plurality of reproduction apparatuses and the encrypted content, and (b) to decrypt the encrypted content

based on the plurality of revocation data read out.

36. **(New)** The copyright protection system according to Claim 35,

wherein each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using a device key held by said plurality of reproduction apparatuses of a corresponding category,

the first plurality of reproduction apparatuses are each configured (a) to hold the plural device keys, (b) to read out, from said recording medium, the corresponding encrypted media key data, the information regarding the generation of the plural device keys, and the encrypted content, (c) to select one among the plural device keys based on the information regarding the generation of the plural device keys, (d) to obtain the media key by decrypting the encrypted media key data using the selected device key, and (e) to decrypt the encrypted content based on the obtained media key, and

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the corresponding encrypted media key data and the encrypted content, (b) to obtain the media key by decrypting the encrypted media key data using the held device key, and (c) to decrypt the encrypted content based on the obtained media key.

37. **(New)** The copyright protection system according to Claim 36,

wherein said recording apparatus is configured to generate an encryption key based on the media key, and to encrypt the content based on the encryption key, and

said plurality of reproduction apparatuses of the respective categories are each configured to generate a decryption key based on the obtained media key, and to decrypt the encrypted content based on the generated decryption key.

38. **(New)** The copyright protection system according to Claim 36,

wherein said recording apparatus is configured to encrypt the content using a content key, to generate encrypted content key data by encrypting the content key using the media key, and to record the generated encrypted content key data onto said recording medium, and

said plurality of reproduction apparatuses of the respective categories are each configured to read out the encrypted content key data from said recording medium, to obtain the content key by decrypting the encrypted content key data using the media key, and to decrypt the encrypted content using the obtained content key.

39. **(New)** The copyright protection system according to Claim 35,

wherein each one of the plurality of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data held by said plurality of reproduction apparatuses of a corresponding category,

said recording apparatus is configured to encrypt the content using a content key, to generate a plurality of encrypted content key data by encrypting the content key using the media keys corresponding to the category of said plurality of reproduction apparatuses, and to record, onto said recording medium, at least encrypted media key data, the information regarding the generations of the plural device keys for encrypting the media key, the plurality of encrypted content key data, and the encrypted content,

the first plurality of reproduction apparatuses are each configured (a) to hold the plural device keys, (b) to read out, from said recording medium, the information regarding the generation of the plural device keys, the encrypted media key data for the corresponding category, the encrypted content key data for the corresponding category, and the encrypted content, (c) to select one among the plural device keys based on the information regarding the generation of the plural device keys, (d) to obtain a media key for the corresponding category by decrypting the encrypted media key data using the selected device key, (e) to obtain the content key by decrypting the encrypted content key data for the corresponding category using the obtained media key for the corresponding category, and (f) to decrypt the encrypted content using the obtained content key, and

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the encrypted media key data for the corresponding category, the encrypted content key data for the corresponding category, and the encrypted content, (b) to obtain the media key for the corresponding category by decrypting the encrypted media key data

using the held device key, (c) to obtain the content key by decrypting the encrypted content key data for the corresponding category using the obtained media key for the corresponding category, and (d) to decrypt the encrypted content using the obtained content key.

40. **(New)** The copyright protection system according to Claim 35,

wherein each of the first plurality of reproduction apparatuses includes:

a read-out apparatus of a second category configured to read out and perform a part of a decryption process on the encrypted content recorded on said recording medium; and

a decryption apparatus of a first category, connected to said read-out apparatus of the second category, configured to perform a part of the decryption process on the encrypted content,

said recording apparatus is configured (a) to generate, based on a media key and on a device key held by each of said decryption apparatus of the first category, a plurality of first revocation data intended for revoking a device key held by a specific decryption apparatus of the first category, (b) to generate, based on a media key and on a device key held by each of apparatuses of the second category, a plurality of second revocation data intended for revoking a device key held by a specific apparatus of the second category, (c) to generate an encrypted content which is the content encrypted based on the media key, and (d) to record at least the plurality of first revocation data, information regarding the generation of the plural device keys for generating the plurality of first revocation data, the plurality of second revocation data, and the encrypted content onto said recording medium,

the second plurality of reproduction apparatuses are each configured to read out the plurality of second revocation data and the encrypted content from said recording medium, and to decrypt the encrypted content based on the plurality of second revocation data read out, and

in each of the first plurality of reproduction apparatuses:

said read-out apparatus of the second category is configured (a) to read out, from said recording medium, the plurality of first revocation data, the information regarding the generations of the plural device keys, the plurality of second revocation data, and the encrypted content, and (to) supply intermediate data, the information regarding the generations of the plural device keys, and the plurality of first revocation data to said decryption apparatus of the first

category, the intermediate data being the encrypted content on which a part of the decryption process has been performed based on the plurality of second revocation data; and

said decryption apparatus of the first category is configured to obtain the content by performing the decryption process on the intermediate data, based on the plurality of first revocation data and the information regarding the generations of the plural device keys supplied by said read-out apparatus of the second category.

41. **(New)** A recording apparatus which encrypts a content and records the encrypted content, the content being reproduced by first reproduction apparatuses which belong to a first category and hold plural device keys and information regarding generations of the plural device keys and by second reproduction apparatuses which belong to a second category and hold only one device key,

wherein said recording apparatus (a) generates, for a plurality of reproduction apparatuses and based on a media key and the device key held by each of the plurality of reproduction apparatuses, a plurality of revocation data intended for revoking a device key held by a specific reproduction apparatus belonging to respective categories, (b) generates an encrypted content which is the content encrypted based on the media key, and (c) records the plurality of revocation data, the information regarding the generations of the plural device keys for generating the plurality of revocation data, and the encrypted content onto a recording medium.

42. **(New)** The recording apparatus according to Claim 41,

wherein each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using the device key held by the plurality of reproduction apparatuses of a corresponding category.

43. **(New)** The recording apparatus according to Claim 42,

wherein said recording apparatus generates an encryption key based on the media key, and encrypts the content based on the encryption key.

44. **(New)** The recording apparatus according to Claim 42,

wherein said recording apparatus encrypts the content using a content key, generates encrypted content key data which is the content key encrypted using the media key, and records the generated encrypted key onto the recording medium.

45. **(New)** The recording apparatus according to Claim 41,

wherein each one of the plurality of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key held by the plurality of reproduction apparatuses of the corresponding category, and

said recording apparatus is configured (a) to encrypt the content using a content key, (b) to generate a plurality of encrypted content key data by encrypting the content key using the media keys corresponding to the category of the reproduction apparatus, and (c) to record, onto the recording medium, at least the encrypted media key data, the information regarding the generations of the plural device keys for encrypting the media key, and the encrypted content.

46. **(New)** The recording apparatus according to Claim 41,

wherein said recording apparatus (a) generates, based on a media key and on a device key held by each of decryption apparatuses of the first category, a plurality of first revocation data intended for revoking a device key held by a specific decryption apparatus of the first category, (b) generates, based on a media key and on a device key held by apparatuses of the second category, a plurality second revocation data intended for revoking a device key held by a specific apparatus of the second category, and (c) generates an encrypted content which is the content encrypted based on the media key, and (d) records at least plurality of first revocation data, information regarding the generations of the plural device keys for generating the plurality of first revocation data, a plurality of the second revocation data, and the encrypted content onto the recording medium.

47. **(New)** A recording medium on which a content reproduced by the plurality of

reproduction apparatuses is recorded, the plurality of reproduction apparatuses including first reproduction apparatuses belonging to a first category and holding plural device keys and information regarding generations of the plural device keys, and second reproduction apparatuses belonging to a second category and holding only one device key,

wherein on said recording medium, at least (i) a plurality of revocation data generated based on a media key and the device key held by each of the plurality of reproduction apparatuses and intended for revoking the device key held by the specific reproduction apparatus of the respective categories, (ii) information regarding generations of the plural device keys for generating the plurality of revocation data, and (iii) an encrypted content generated by encrypting the content based on the media key are recorded.

48. **(New)** The recording medium according to Claim 47,

wherein each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using the device key held by the plurality of reproduction apparatuses of a corresponding category.

49. **(New)** The recording medium according to Claim 48,

wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key.

50. **(New)** The recording medium according to Claim 48,

wherein the encrypted content is generated by encrypting the content using a content key, and

on said recording medium, encrypted content key data is recorded, the encrypted content key data being generated by encrypting the content key using the media key.

51. **(New)** The recording medium according to Claim 47,

wherein each one of the plurality of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key held by the plurality of

reproduction apparatuses of the corresponding category,

the encrypted content is generated by encrypting the content using a content key, and

on said recording medium, a plurality of encrypted content key data generated by encrypting the content key using the media keys corresponding to the category of the plurality of reproduction apparatuses are recorded.

52. **(New)** The recording medium according to Claim 47,

wherein on said recording medium, at least (i) a plurality of first revocation data generated based on the media key and on plural device keys held by decryption apparatuses of the first category and intended for revoking a device key held by a specific decryption apparatus of the first category, (ii) information regarding generations of the plural device keys for generating the plurality of first revocation data, (iii) a plurality of second revocation data generated based on a media key and on plural device keys held by apparatuses of the second category and intended for revoking a device key held by a specific apparatus of the second category, and (iv) the encrypted content which is the content on which an encryption process has been performed based on the media key are recorded.

53. **(New)** A reproduction apparatus which belongs to one of plural categories and reproduces an encrypted content recorded on a recording medium,

wherein on the recording medium, at least revocation data generated based on a media key and a device key held by said reproduction apparatus and intended for revoking the device key held by said reproduction apparatus, an encrypted content generated by encrypting a content based on the media key, and information regarding generations of the plural device keys for generating the revocation data, and

said reproduction apparatus (a) reads out, from the recording medium, the revocation data, corresponding to said reproduction apparatus, the information regarding the generations of the plural device keys, and the encrypted content, and (b) decrypts the encrypted content based on the plurality of revocation data read out and the information regarding the generations of the plural device keys.

54. **(New)** The reproduction apparatus according to Claim 53,

wherein the revocation data is encrypted media key data which is the media key encrypted using the device key data held by said reproduction apparatus, and

said reproduction apparatus (a) holds plural device keys, (b) reads out, from the recording medium, the encrypted media key data, the information regarding the generations of the plural device keys, and the encrypted content, (c) selects one among the plural device keys based on the information regarding the generations of the plural device keys, (d) obtains the media key by decrypting the encrypted media key data using the selected device key, and (e) decrypts the encrypted content based on the obtained media key.

55. **(New)** The reproduction apparatus according to Claim 54,

wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key, and

said reproduction apparatus generates a decryption key based on the obtained media key, and decrypts the encrypted content based on the generated decryption key.

56. **(New)** The reproduction apparatus according to Claim 54,

wherein the encrypted content is generated by encrypting the content using a content key,

on the recording medium, encrypted content key data generated by encrypting the content key using the media key is recorded, and

said reproduction apparatus (a) reads out the encrypted content key data from the recording medium, (b) obtains the content key by decrypting the encrypted content key data using the media key, and (c) decrypts the encrypted content using the obtained content key.

57. **(New)** The reproduction apparatus according to Claim 53,

wherein the revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key held by said reproduction apparatus,

the encrypted content is generated by encrypting the content using a content key,

on the recording medium, encrypted content key data generated by encrypting the content key using the media keys corresponding to the category of said reproduction apparatus is recorded, and

said reproduction apparatus (a) holds plural device keys, (b) reads out, from the recording medium, the encrypted media key data for the corresponding category, the encrypted content key data for the corresponding category, the encrypted content, and the information regarding the generations of the plural device keys (c) selects one among the plural device keys based on the information regarding the generations of the plural device keys, (d) obtains the media key for the corresponding category by decrypting the encrypted media key data using the selected device key, (e) obtains the content key by decrypting the encrypted content key data using the obtained media key for the corresponding category, and (f) decrypts the encrypted content using the obtained content key.

58. **(New)** The reproduction apparatus according to Claim 53,

wherein on the recording medium, at least (i) a plurality of first revocation data generated based on the media key and on a device key held by each of decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, (ii) information regarding generations of the plural device keys for generating the plurality of first revocation data, (iii) a plurality of second revocation data generated based on a media key and on a device key held by each of apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category, and (iv) the encrypted content which is the content on which an encryption process has been performed based on the media key are recorded, and

said reproduction apparatus belongs to the second category and reads out, from the recording medium, the plurality of second revocation data and the encrypted content, and decrypts the encrypted content based on the plurality of second revocation data.

59. **(New)** The reproduction apparatus according to Claim 58, comprising:

a read-out apparatus belonging to the second category and configured to read out, from

the recording medium, the plurality of first revocation data, the plurality of second revocation data, the information regarding the generations of the plural device keys, and the encrypted content, to generate intermediate data which is the encrypted content on which a part of a decryption process has been performed based on the plurality of second revocation data, and to output the generated intermediate data, the information regarding the generations of the media keys, and the first revocation; and

a decryption apparatus belonging to the first category and configured to obtain the content by performing a decryption process on the intermediate data, based on the plurality of first revocation data and the information regarding the generations of the plural device keys.

60. **(New)** A copyright protection system comprising:

a key generation apparatus configured to generate and record a plurality of revocation data necessary for encrypting and decrypting a content,

a plurality recording apparatuses, each of which is configured to encrypt a content and to record the encrypted content;

a recording medium on which the encrypted content and the plurality of revocation data are recorded; and

a plurality of reproduction apparatuses, each of which is configured to read out and decrypt the encrypted content recorded on said recording medium,

wherein each of said plurality of reproduction apparatuses is one of either first reproduction apparatuses which belong to a first category and hold plural device keys and information regarding generations of the plural device keys or second reproduction apparatuses which belong to a second category and hold only one device key,

each of said plurality recording apparatuses belongs to either the first category or the second category,

said key generation apparatus is configured (a) to generate, for said plurality of reproduction apparatuses and based on a media key and the device key held by each of said plurality recording apparatuses or plurality of reproduction apparatuses, the plurality of

revocation data intended for revoking a device key held by a specific recording apparatus or a specific reproduction apparatus of the respective categories, and (b) to record the generated a plurality of revocation data and the information regarding the generations of the plural device keys for generating the plurality of revocation data onto said recording medium,

said plurality recording apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data for the category to which said recording apparatus belongs, (b) to generate the encrypted content by encrypting the content based on the plurality of revocation data read out, and (c) to record the generated encrypted content on said recording medium,

the first reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said first reproduction apparatus, the information regarding the generations of the plural device keys, and the encrypted content, and (b) to decrypt the encrypted content based on the plurality of revocation data read out and the information regarding the generations of the plural device keys, and

the second reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said second reproduction apparatus and the encrypted content, and (b) to decrypt the encrypted content based on the plurality of revocation data read out.

61. **(New)** A recording method for use in a recording apparatus which encrypts a content reproduced by plurality of reproduction apparatuses and records the encrypted content, the plurality of reproduction apparatuses including first reproduction apparatuses belonging to a first category and holding plural device keys and information regarding generations of the plural device keys, and second reproduction apparatuses belonging to a second category and holding only one device key, said method comprising:

a step of generating, for the plurality of reproduction apparatuses and based on a media key and the device key held by each of said plurality of reproduction apparatuses, a plurality of revocation data intended for revoking a device key held by a specific reproduction apparatus of the respective categories;

an encrypted content generation step of generating the encrypted content by encrypting the content, based on the media key; and

a recording step of recording the plurality of revocation data, the information regarding the generations of the plural device keys for generating the plurality of revocation data, and the encrypted content onto the recording medium.

62. **(New)** A reproduction method for use in a reproduction apparatus which belongs to one of plural categories and reproduces an encrypted content recorded on a recording medium,

wherein on the recording medium, at least the plurality of revocation data generated based on a media key and a device key held by the reproduction apparatus and intended for revoking the device key held by the reproduction apparatus, the encrypted content generated by encrypting a content based on the media key, and information regarding generations of the plural device keys are record, and

said reproduction method comprises:

a read-out step of reading out, from the recording medium: the plurality of revocation data corresponding to the reproduction apparatus; the information regarding the generations of the plural device keys; and the encrypted content; and

a decryption step of decrypting the encrypted content based on the plurality of revocation data read out and the information regarding the generations of the plural device keys.